UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JUAN ANAYA, STEVEN BETTS, WILLIAM COOK, AMBER HORNICK, CAROLYN PLUHAR, KYLE REYNOLDS, and VIRGINIA ROMANO, individually and on behalf of all OTHERS similarly situated, Plaintiffs, v. CENCORA, INC.; THE LASH GROUP, LLC; SUMITOMO PHARMA AMERICA, INC.; BRISTOL MYERS SQUIBB COMPANY; and BRISTOL MYERS SQUIBB PATIENT ASSISTANCE FOUNDATION, INC.; REGENERON PHARMACEUTICALS, INC.; GLAXOSMITHKLINE, LLC; GLAXOSMITHKLINE PATIENT ACCESS PROGRAMS FOUNDATION, Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

COMPLAINT – Class Action

Plaintiffs Juan Anaya, Steven Betts, William Cook, Amber Hornick, Carolyn Pluhar, Kyle Reynolds, and Virginia Romano (collectively, "Plaintiffs"), by and through undersigned counsel, bring this class action on behalf of themselves and all others similarly situated (the "Class," defined more fulsomely below) against Defendants Cencora, Inc. ("Cencora"); The Lash Group, LLC ("Lash Group"); Sumitomo Pharma America, Inc. ("Sumitomo"); Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc. (collectively, "BMS"); Regeneron Pharmaceuticals, Inc. ("Regeneron"); GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation (collectively, "GSK") (all collectively, "Defendants").

Plaintiffs make the following allegations based on personal knowledge as to their own actions and on information and belief as to all other matters.

NATURE OF THE ACTION

1. Cencora, formerly known as AmerisourceBergen, is a pharmaceutical giant that brings in over $230 billion in annual revenue. According to Fortune, it was the 24th largest corporation on the planet in 2023 and in 2024 was 10th largest corporation in the United States of America. With its over 46,000 employees, Cencora provides services related to drug distribution, specialty pharmacy, consulting, and clinical trial support.[1] Despite its wealth and influence, Cencora allowed computer hackers to make off with intimate medical information concerning Plaintiffs and millions of Class Members.

2. Lash Group, a division of Cencora, specializes in patient support technologies. Cencora and Lash Group (collectively, "Cencora") work with pharmaceutical firms, healthcare providers, and pharmacies to offer drug distribution, patient support services, business analytics, and other services.[2]

3. On February 27, 2024, Cencora disclosed in an SEC filing that it failed to prevent computer hackers from infiltrating its systems and stealing sensitive information (the "Data Breach"). The SEC filing confirmed that "[o]n February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which may contain personal information."[3]

---

[1] *Cencora Reports Fiscal 2024 First Quarter Results*, CENCORA (Jan. 31, 2024), https://investor.cencora.com/news/news-details/2024/Cencora-Reports-Fiscal-2024-First-Quarter-Results.

[2] The Lash Group, https://www.lashgroup.com/#:~:text=We%20pair%20advanced%20technologies%20with,every%20step%20of%20the%20way (last visited June 20, 2024).

[3] Cencora, Inc. (Feb. 27, 2024) *Form 8-K*, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001140859/81c828c1-699f-45d0-a610-e985f8e8c4b9.pdf [hereinafter, "*SEC Filing*"].

4. While many consumers have never heard of Cencora, this pharmaceutical behemoth serves more than 18 million patients and handles approximately 20% of the pharmaceuticals distributed across the United States, operating largely behind the scenes in its work with many of the largest pharmaceutical companies including Bristol Myers Squibb, GlaxoSmithKline, Regeneron, and Sumitomo.

5. Cencora has not yet confirmed the total number of either individuals or its pharmaceutical company partners that were affected by its Data Breach but public reports indicate that the Data Breach included information from at least 24 pharmaceutical and biotechnology companies[4] and over 540,000 impacted individuals have been notified.[5]

6. In May and June of 2024, many among Plaintiffs and Class members learned of Cencora for the first time when they received a letter notifying them that their information had been impacted in a Data Breach months prior. The letters indicated that Cencora had learned of the Breach on February 21, 2024 and completed its investigation on April 10, 2024. This

[4] Based on notifications sent to state Attorneys General thus far, the list of impacted companies includes: Abbot; AbbVie Inc.; Acadia Pharmaceuticals Inc.; Amgen Inc.; Bausch Health Companies Inc.; Bayer Corporation; Bristol Myers Squibb Company; Bristol Myers Squibb Patient Assistance Foundation; Dendreon Pharmaceuticals LLC; Endo Pharmaceuticals Inc.; Genentech, Inc.; GlaxoSmithKline Group of Companies; GlaxoSmithKline Patient Access Programs Foundation; Heron Therapeutics, Inc.; Incyte Corporation; Johnson & Johnson Services, Inc.; Johnson & Johnson Patient Assistance Foundation, Inc.; Marathon Pharmaceuticals, LLC/PTC Therapeutics, Inc.; Novartis Pharmaceuticals Corporation; Otsuka America Pharmaceutical, Inc.; Pfizer Inc.; Pharming Healthcare, Inc.; Rayner Surgical Inc. Regeneron Pharmaceuticals, Inc; Sandoz Inc.; Sumitomo Pharma America, Inc. / Sunovion Pharmaceuticals Inc.; Takeda Pharmaceuticals U.S.A., Inc.; and Tolmar.

[5] Alicia Hope, *Pharmaceutical Giant Cencora Confirms Patient Data Breach Impacting over a Dozen Pharma Companies* (May 31, 2024), CPO MAGAZINE, https://www.cpomagazine.com/cyber-security/pharmaceutical-giant-cencora-confirms-patient-data-breach-impacting-over-a-dozen-pharma-companies/#:~:text=Over%20540%2C000%20victims%20notified%20in,distributed%20across%20the%20United%20States.

investigation concluded that the stolen information could include names, addresses, dates of birth, diagnosis information, and medication or prescription information.

7. While Defendants have not yet disclosed the precise extent of the data accessed and exfiltrated amid this attack, the circumstances and the information released thus far indicate the unauthorized disclosure of Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (together, "Private Information").

8. While letters received by some Plaintiffs and Class members identified the pharmaceutical company through which Cencora had received patients' and customers' personal information, the majority—including Defendant Regeneron—have declined to reveal themselves to the customers whose information they were responsible for.[6]

9. Defendants systemically collected and maintained vast amounts of Private Information about millions of customers and patients. These individuals, including Plaintiffs and Class members, entrusted Defendants with their most sensitive data with the mutual understanding that it would be protected against disclosure. Instead, Defendants' negligence has put millions of current and former customers and patients at lifelong risk of identity theft and fraud.

10. Defendants owed a non-delegable duty to Plaintiffs and Class members to implement reasonable and adequate security measures to protect their Private Information. Yet, Defendants maintained and shared the Private Information in a negligent and/or reckless manner.

[6] BMS, GSK, Novartis Pharmaceuticals Corporation, and Sumitomo Pharma America, Inc./ Sunovion Pharmaceuticals Inc. have all sent letters identifying themselves as the company through or on behalf of which Cencora and Lash Group received the patient's information. The majority of the affected companies have hidden behind letters that identify only Cencora and Lash Group by name and refer to the individual pharmaceutical company as only "one such organization."

In particular, Private Information was maintained on computer systems in a condition vulnerable to cyberattacks that lacked, for example, multi-factor authentication to access.

11. After numerous high-profile cyberattacks across the healthcare industry in recent years and numerous warnings by government agencies, such a data breach was a known risk to Defendants. Still, Defendants failed to take the necessary steps to secure Plaintiffs' Private Information.

12. Plaintiffs' and Class members' Private Information was compromised due to Defendants' negligent and/or reckless acts and omissions and Defendants' repeated failure to reasonably and adequately protect Plaintiffs' and Class members' Private Information.

13. As a result of the Data Breach, Plaintiffs and Class members suffered concrete injuries in fact including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains inadequately secured and vulnerable to unauthorized access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

14. Cybercriminals can (and almost certainly will) distribute Plaintiffs' and Class Members' Private Information from the Data Breach in illicit underground marketplaces, including on the Dark Web. The information will be used to harm Plaintiffs and Class members in a variety of ways including: destroying their credit and leaving them financially liable by

opening new financial accounts and taking out loans in their names; improperly obtaining medical services and pharmaceuticals; facilitating other phishing and hacking intrusions; and impersonating them to obtain benefits; and otherwise assuming their identities.

15. As a result of the Data Breach, Plaintiffs and Class members face a substantial and imminent risk of harm relating to the exposure and misuse of their Private Information. Plaintiffs and Class members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

16. Plaintiffs initiate this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class members' Private Information, which they collected and maintained.

17. Further, Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

18. Plaintiff Juan Anaya is, and was at all relevant times, an adult and a citizen of Illinois, residing in Tinley Park, Illinois.

19. Plaintiff Steven Betts is, and was at all relevant times, an adult and a citizen of North Carolina, residing in Fayetteville, North Carolina.

20. Plaintiff William Cook is, and was at all relevant times, an adult and a citizen of Idaho, residing in Post Falls, Idaho.

21. Plaintiff Amber Hornick is, and was at all relevant times, an adult and a citizen of Georgia, residing in Marietta, Georgia.

22. Plaintiff Carolyn Pluhar is, and was at all relevant times, an adult and a citizen of Montana, residing in Billings, Montana.

23. Plaintiff Kyle Reynolds is, and was at all relevant times, an adult and a citizen of North Carolina, residing in Charlotte, North Carolina.

24. Plaintiff Virginia Romano is, and was at all relevant times, an adult and a citizen of Indiana, residing in Elkhart, Indiana.

25. Defendant Cencora, Inc. is a Delaware corporation with its principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

26. Defendant The Lash Group LLC is a Delaware limited liability company with a principal place of business located at 1 West First Avenue, Conshohocken, Pennsylvania 19428. Lash Group's sole member is AmerisourceBergen Consulting Services, LLC, a Delaware limited liability company. AmerisourceBergen Consulting Services, LLC's sole member is AmerisourceBergen Drug Corporation, a Delaware corporation whose principal place of business also is located at 1 West First Avenue, Conshohocken, Pennsylvania 19428. Finally, AmerisourceBergen Drug Corporation's sole shareholder in turn is Defendant Cencora, Inc. The Lash Group is a citizen of each State in which its member is a citizen. The Lash Group is therefore a citizen of the Commonwealth of Pennsylvania and the State of Delaware. The Lash Group is a patient support company, owned by Defendant Cencora, that provides patient support services, business analytics and technology services, and other services to pharmaceutical companies, pharmacies, and other healthcare providers.

27. Defendant Sumitomo Pharma America, Inc.—formerly known as Sunovion Pharmaceuticals Inc.—is a Delaware corporation with a principal place of business at 55 Cambridge Parkway, Suite 102W, Cambridge, Massachusetts 02142.

28. Defendant GlaxoSmithKline, LLC, is a Delaware corporation with its headquarters located at 2929 Walnut St., Suite 1700, Philadelphia, Pennsylvania 19104.

29. Defendant GlaxoSmithKline Patient Access Programs Foundation is a 501(c)(3) non-profit with its headquarters located at 2929 Walnut St., Suite 1700, Philadelphia, Pennsylvania 19104.

30. Defendant Regeneron Pharmaceuticals, Inc. is a New York corporation with its principal place of business at 777 Old Saw Mill River Road, Tarrytown, NY 10591.

31. Defendant Bristol Myers Squibb Company is a Delaware corporation with its principal place of business at Route 206 & Province Line Road Princeton, New Jersey.

32. Defendant Bristol Myers Squibb Patient Assistance Foundation, Inc. is a 501(c)(3) non-profit with its principal place of business at Route 206 & Province Line Road Princeton, New Jersey.

JURISDICTION AND VENUE

33. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the proposed Class) are citizens of states different from Defendants.

34. This Court has jurisdiction over Defendants because Defendants Cencora, Lash Group, and GSK operate their principal places of business within this District, indicating a deliberate engagement with the markets here, and all Defendants (including BMS, Regeneron, and Sumitomo) operate in and direct commerce within this District. Consequently, the exercise

of jurisdiction by this Court is not only justified but also appropriate, given Defendants' intentional involvement in this District's economic activities.

35. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants Cencora, Lash Group, and GSK maintain their principal places of business in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendants' Business

36. Defendant Cencora—formerly known as AmerisourceBergen[7]—is a leading pharmaceutical solutions organization that provides "end-to-end pharmaceutical commercialization solutions" and claims to "empower[] patient-centered care all over the world.[8] Cencora "connects manufacturers, providers, pharmacies, and patients" to provide drug distribution and consulting services.[9]

37. Defendant Lash Group, a subsidiary of Cencora,[10] "partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support and services, business analytics and technology, and other services."[11]

---

[7] *See AmerisourceBergen becomes Cencora, in alignment with the company's growing global footprint and central role in pharmaceutical access and care*, CENCORA (Aug. 30, 2023), https://www.cencora.com/newsroom /amerisourcebergen-becomes-cencora (last accessed July 2, 2024).

[8] *Who we are*, CENCORA, https://www.cencora.com/who-we-are (last accessed June 20, 2024).

[9] *What we offer*, CENCORA, https://www.cencora.com/what-we-offer (last accessed June 20, 2024).

[10] *See Our Network*, LASH GROUP, https://www.lashgroup.com/our-network (last accessed June 20, 2024).

[11] *Notice of Data Security Incident*, LASH GROUP, https://www.lashgroup.com/notice (last accessed June 20, 2024) [hereinafter, the "*Website Notice*"].

38. Defendant Bristol Myers Squibb Company is "a global biopharmaceutical company whose mission is to discover, develop and deliver innovative medicines that help patients prevail over serious diseases."[12]

39. Defendant Bristol Myers Squibb Patient Assistance Foundation is an independent charitable organization that provides certain Bristol Myers Squibb medicines to eligible patients free of charge.[13]

40. Defendant GlaxoSmithKline, LLC is the United States operation of GSK, Plc, a global biopharma company that develops vaccines, specialty and general medicines.[14]

41. Defendant GlaxoSmithKline Patient Access Programs Foundation is operated by GlaxoSmithKline and provides medications and vaccinations at no or reduced cost to persons meeting certain criteria.[15]

42. Defendant Regeneron is "a leading biotechnology company that invents, develops, and commercializes life-transforming medicines for people with serious diseases."[16]

43. Defendant Sumitomo is "a science-based, technology-driven biopharmaceutical company focused on delivering therapeutic and scientific breakthroughs in areas of critical patient need in psychiatry and neurology, oncology, urology, women's health, rare disease, and cell and gene therapies." It was formed through the consolidation of Japanese multinational pharmaceutical company Sumitomo Pharma's U.S. affiliate companies including Sunovion

---

[12] *About Us*, BRISTOL MYERS SQUIBB, https://www.bms.com/about-us.html (last visited June 20, 2024).
[13] *What is the Bristol Myers Squibb Patient Assistance Foundation*, Bristol Myers Squibb Patient Assistance Foundation, https://www.bmspaf.org/#/about (last visited June 20, 2024).
[14] *Purpose, strategy, and culture*, GSK, https://us.gsk.com/en-us/company/purpose-strategy-and-culture/ (last accessed June 20, 2024).
[15] *GSK Patient Assistance Programs*, GSK, https://www.gskforyou.com/content/dam/cf-pharma/gskforyou/master/pdf/GSK-PAP-Information-Sheet.pdf (last accessed June 20, 2024).
[16] *About*, Regeneron, https://www.regeneron.com/about (last accessed June 20, 2024).

Pharmaceuticals, Inc., Sumitomo Pharma America Holdings, Inc., Sumitomo Pharma Oncology, Inc., Sumitovant Biopharma, Inc., Myovant Sciences, Inc., Urovant Sciences, Inc. and Enzyvant Therapeutics, Inc.[17]

44. In the regular course of their business, including through operating their patient assistance programs, BMS, GSK, Regeneron, and Sumitomo (collectively, "Drug Company Defendants") collect and maintain the Private Information of their current and former customers. Drug Company Defendants, either directly or indirectly, required Plaintiffs and Class members to provide their Private Information as a condition of receiving pharmaceutical services, special prices for pharmaceuticals, or other benefits.

45. Drug Company Defendants shared Plaintiffs' and Class members' Private Information with Cencora and Lash Group in connection with obtaining services from Cencora and Lash Group.

46. Alternatively, Cencora—acting on behalf of the Drug Company Defendants and other pharmaceutical companies to provide services to Plaintiffs and Class members on behalf of those companies—collected, processed, and stored Plaintiffs' and Class members Private Information.

47. This Private Information was highly sensitive and included some or all of the following:

a. Full names and addresses;

b. Personal email addresses and phone numbers;

c. Dates of birth;

[17] Sumitomo Pharma America, Inc., LinkedIn Profile, https://www.linkedin.com/company/sumitomo-pharma-america/about/ (last accessed June 20, 2024).

d. Social Security numbers;

e. Driver's licenses (or other similar state identifications);

f. Health insurance information;

g. Health information, including diagnoses, prescriptions, personal medical histories, family medical histories, mental health information, STD status and treatment, contraceptive use, and information about patients' obtaining abortion services;

h. Information about physicians and related medical professionals involved in prior or ongoing treatment of the individual;

i. Billing and claims information, including credit and debit card numbers, bank account statements, account numbers, and insurance payment details; and

j. Medicare/Medicaid information.

48. This sort of Private Information is extremely sensitive and is highly valuable to criminals because it can be used to commit identity theft and medical theft crimes.

49. Because of the highly sensitive and personal nature of the information about Plaintiffs and Class members that Defendants collect, process, and store, Defendants are obligated to, among other things: keep Private Information private; comply with data security standards applicable within the healthcare industry, including FTC guidelines; and comply with all applicable federal and state laws protecting consumer Private Information.

50. As HIPAA-covered business entities, as discussed *infra*, Defendants are required to implement and maintain adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing the requirements of the HIPAA Security Rule.

Defendants' Privacy Policies and Practices

51. Cencora's website states, "Cencora, Inc. and its affiliate companies ("Cencora") value and protect the personal information entrusted to the company by its suppliers, customers, and visitors. As a United States company doing business around the world, Cencora maintains a comprehensive privacy program designed to comply with its legal obligations under applicable law."[18]

52. Lash Group's website contains a Notice of Privacy Practices (the "Privacy Policy") that "describes how Lash Group may use and disclose your health information."[19] This includes for treatment, payment, and healthcare operations, among others.[20]

53. Lash Group admits it is required by law to follow the Privacy Policy and further admits it is required by law to maintain the privacy of PHI.[21]

54. The Privacy Policy promises "Lash Group respects the confidentiality of your health information and will protect it in a responsible and professional manner."[22]

55. According to the Privacy Policy, Lash Group is required to "obtain your written authorization to use or disclose your health information for reasons other than those listed [in the Privacy Policy] and permitted under law."[23]

[18] *Privacy Statement Overview*, CENCORA, https://www.cencora.com/global-privacy-statement-overview (last accessed June 20, 2024).
[19] *Notice of Privacy Practices*, LASH GROUP (July 1, 2012), https://www.lashgroup.com/notice-of-privacy-practices.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*

56. BMS's website states that, for BMS, "data privacy goes beyond mere compliance with the law." It promises that "BMS employs reasonable and appropriate security measures." Its policy states:

> We implement appropriate technical and organizational controls to protect your Personal Information that we hold to prevent unauthorized Processing, loss of data, disclosure, use, alteration, or destruction. Where appropriate, we use encryption, pseudonymisation (such as key coding), de-identification and other technologies that can assist us in securing the information about you, including measures to restore access to your information. We also require our service providers to comply with reasonable and recognized data privacy and security requirements.
>
> We conduct tests and reviews of our technologies and processes, including a review of our business partners and vendors, so that our security controls remain effective. Also, we may further anonymize your Personal Information when it is no longer needed for the purpose for which BMS originally collected such Information. [24]

57. BMS concedes that it shares consumer information with third-parties, and states that "[w]hen doing so, we implement appropriate measures to prevent unauthorized access or Use of your Personal Information."[25]

58. GSK's website lists its Privacy Principles, which include "Be secure." GSK states, "We respect the privacy of our patients …. We inspire trust and are thoughtful when we use personal information." GSK promises to "protect personal information by implementing appropriate safeguards."[26]

---

[24] *Privacy Notice Center*, BRISTOL MYERS SQUIBB, https://www.bms.com/privacy-policy.html (last accessed June 20, 2024).
[25] *Id.*
[26] *GSK's Privacy Principles*, GSK, https://privacy.gsk.com/en-us/privacy-notice/privacy-principles/ (last accessed June 20, 2024).

59. GSK claims it will only "keep your personal information for as long as needed or permitted for the purpose(s) described in this privacy policy and consistent with applicable law."[27]

60. GSK promises it will only "share your personal information on a need-to-know basis, to the extent necessary to follow laws and regulations, and to manage the activities related to our relationship with you." GSK further claims: "In some cases, our relationship with you is supported by specialized service providers working on our behalf. These service providers are contractually-required to protect your personal information and not to use it for their own purposes."[28]

61. GSK pledges it "will take appropriate legal, organizational, and technical measures to protect your personal information."[29]

62. GSK acknowledges the "need to keep GSK's information and data secure from increasingly sophisticated cyber-attacks and technology misuse." GSK also acknowledges it is responsible for "protecting GSK data that contains information on patients, customers, and employees."[30]

63. Regeneron's website states that Regeneron (including its subsidiaries and affiliates) "is committed to respecting your privacy." [31]

64. Regeneron, too, concedes that it shares patient and consumer information with third-parties. In relevant part, the Regeneron's privacy policy states:

---

[27] *GSK US Privacy Notice,* GSK, https://privacy.gsk.com/en-us/privacy-notice/ (last accessed July 2, 2024).
[28] *Id.*
[29] *Id*.
[30] GSK Policies and Standards, https://www.gsk.com/media/8518/policies-and-standards.pdf (last accessed July 2, 2024)
[31] *Privacy Notice*, REGENERON, https://www.regeneron.com/privacy-notice (last accessed June 20, 2024).

> If you are a participant in a United States … Regeneron patient support program, we may collect and process additional categories of Personal Data about you, which we received directly from you, your healthcare provider (HCP), payor, and related third parties. With your written consent provided in the related patient support program enrollment form, we use and disclose your Personal Data to administer and manage the patient support program, facilitating benefit verification, to conduct HCP follow-up, safety monitoring, and to comply with applicable laws and regulations. We will also de-identify your Personal Data so that it does not directly identify you for the following purposes: analytics, research and publication, development and improvement of Regeneron's programs and related services, products and medicines.[32]

65. Regeneron's policy is to retain Private Information "for the period necessary fulfill the legitimate business purposes or uses outlined in this Privacy Notice, unless a longer retention period is required or allowed by applicable data protection law or to otherwise fulfill a legal obligation."[33]

66. Sumitomo also concedes that it shares Private Information (which it defines as "Personal Data") with third parties. The privacy policy on its website states "We will try to assure that no information that is transferred will be used or shared in a manner inconsistent with this notice without your consent."[34]

67. Sumitomo promises that it "maintain[s] reasonable technical, administrative and procedural measures to protect your information from unauthorized access or use."[35]

68. Despite what Defendants promise in their policies, and despite the existence of their legal and equitable duties to protect Plaintiffs' and Class members' Private Information,

---

[32] *Id.*
[33] *Id.*
[34] *Sumitomo Pharma America, Inc. Privacy & Cookie Notice*, SUMITOMO PHARMA, https://www.us.sumitomo-pharma.com/privacy-notice/ (last accessed June 20, 2024).
[35] *Id.*

Defendants did not maintain adequate security to protect their systems from infiltration by cyber criminals.

69. Plaintiffs and the Class members trusted these assurances and counted on these sophisticated business entities to maintain the confidentiality and security of their sensitive Private Information. They expected Defendants to use this information solely for business purposes and to make only authorized disclosures. Plaintiffs and Class members, in general, insist on security measures to protect their Private Information, particularly when it involves sensitive details like Social Security numbers.

The Data Breach

70. On February 27, 2024, Cencora filed a Form 8-K with the SEC disclosing that it had failed to prevent a data breach that resulted in the theft of sensitive information. The SEC filing confirmed that "[o]n February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which may contain personal information."[36]

71. Cencora began sending out letters to impacted individuals in May 2024. The breach notice letters received by Plaintiffs indicate that the investigation into the Data Breach determined that personal information was impacted, including patients' names, addresses, dates of birth, health diagnoses, and medication or prescription information.

72. Cencora's Form 8-K filing omits crucial information including the date(s) on which the Data Breach actually occurred, how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the two-month delay in notifying Plaintiffs and Class members of the Data Breach, how it determined that the Personal Information had been accessed, and of particular importance

[36] *SEC Filing, supra* n.3.

to Plaintiffs and Class members, what actual steps Cencora took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks. To this day, these critical details have not been explained or clarified to Plaintiffs and Class members, who maintain a vested interest in safeguarding their Private Information. Without such essential details, the ability of Plaintiffs and Class members to effectively mitigate the resulting harms is significantly limited.

73. Despite the intentional opacity from Cencora regarding the details of this incident, the SEC filing and the subsequent breach notice letters sent to Plaintiffs provide several discernable facts: a) the Data Breach was perpetrated by cybercriminals; b) these cybercriminals initially breached Cencora's networks and systems before exfiltrating data; c) within Cencora's networks and systems, the cybercriminals specifically targeted information—such as Plaintiffs' and Class members' PHI, PII, and other sensitive data—for download and theft.

74. The information compromised in the Data Breach included Plaintiffs' and Class members' PII and PHI, as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

75. As detailed further below, Defendants were bound by obligations stemming from the FTC Act, HIPAA, contractual agreements, common law principles, and industry standards to maintain the confidentiality of Plaintiffs' and Class members' Private Information and safeguard it against unauthorized access and disclosure.

76. Defendants failed to implement reasonable security procedures and practices commensurate with the sensitivity of the information they held concerning Plaintiffs and Class members. This lapse led to the exposure of Private Information, which could have been mitigated through reasonable and adequate information security controls.

77. The hackers successfully accessed and obtained unencrypted Private Information of Plaintiffs and Class members.

78. Based on the hackers intentionally targeting Plaintiffs' and Class members' Private Information, the Cencora Data Breach likely was carried out by a financially motivated hacking group. The modus operandi of such hacking groups would be to distribute Plaintiffs' and Class members' Private Information through illicit criminal networks, possibly including on the dark web.

Defendants Acquired, Collected, and Stored Patients' Private Information

79. Defendants all acquire, collect, and store massive amounts of Private Information on their current and former patients and customers as a routine part of their business.

80. As a condition of receiving medications, financial assistance, and other healthcare related services, Plaintiffs and Class members were required to entrust Drug Company Defendants and/or Cencora on the Drug Company Defendants' behalf with highly sensitive personal information.

81. Defendants, in turn, entrusted Plaintiffs' and Class members Private Information to Cencora and Lash Group.

82. By directly or indirectly collecting, processing, and storing Plaintiffs' and Class members' Private Information, Defendants each assumed legal and equitable duties to protect such information. Each Defendant knew or should have known that it was responsible for protecting this Private Information from disclosure.

83. Plaintiffs and Class members would not have entrusted their Private Information to Defendants absent a promise to safeguard this information from unauthorized disclosure.

84. Plaintiffs and Class members relied on Defendants to keep their Private Information confidential and securely maintained.

85. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement and maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

86. The ramifications of Defendants' failure to properly secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and resulting damage to victims may continue for years.

87. As healthcare industry entities in custody of Plaintiffs' and Class members' Private Information, Defendants knew or should have known the importance of safeguarding the Private Information in their possession, custody, or control, and of the foreseeable consequences of their data security systems being breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Plaintiffs' Private Information Has Value

88. Criminal actors highly value PHI and PII. Such information is continually traded on underground marketplaces, including on the dark web, a section of the internet that cannot be accessed through standard web browsers.

89. Private Information can be sold at a price ranging from $40 to $200 per individual.[37] Medical records are valued at between $1 and $1,000 per individual depending on completeness.[38]

90. The kind of information likely exposed in the Data Breach poses a significant risk to Plaintiffs and Class members. Unlike data breaches that involve credit card information, the information taken in the Cencora data breach cannot be changed because it involves immutable personal characteristics.

91. Social Security numbers—which, according to available information, were almost certainly compromised in the Data Breach—are one of the most detrimental forms of Private Information to have stolen due to the multitude of fraudulent purposes for which they can be used and the significant challenge individuals face in changing them.

92. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[39] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[40]

93. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the

[37] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[38] *Id.*
[39] *See Avoid Identity Theft: Protect Social Security Numbers,* SOC. SEC. PHILA. REG., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited June 7, 2024).
[40] *Id.*

possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

94. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[41]

95. Theft of PHI, which, upon information and belief, was compromised in the Data Breach, is also gravely serious, putting patients at risk of medical identity theft wherein "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

96. A study conducted by Experian revealed that the average cost of medical identity theft for victims per incident is approximately $20,000. Additionally, the majority of victims of medical identity theft are compelled to cover out-of-pocket expenses for healthcare services they did not receive in order to reinstate their coverage. Furthermore, almost half of medical identity theft victims lose their healthcare coverage following the incident, while nearly one-third experience an increase in insurance premiums. Alarmingly, 40 percent of victims are unable to fully resolve their identity theft ordeal.[43]

---

[41] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

[42] *Medical I.D. Theft*, EFRAUDPREVENTION, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited June 7, 2024).

[43] *The Truth Behind Medical Identity Theft: What You Don't Know Can Cost You,* , EXPERIAN, (March 3, 2010), https://www.experianplc.com/newsroom/press-releases/2010/the-truth-behind-medical-identity-theft-what-you-don-t-know-can-cost-you.

97. Fraudulent medical treatment also has non-financial impacts. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because their medical records contain information supplied by an individual obtaining treatment under a false name.[44]

98. Further, loss of personal health information, such as treatment history, diagnoses, and prescription information, exposes the victims to loss of reputation, loss of employment, blackmail, and other harms including the trauma of having their most personal details published online for all to see.

99. PII also sells on legitimate markets, an industry that is valued at hundreds of billions of dollars per year. Customers themselves are able to sell non-public information directly to data brokers who aggregate the information for sale to marketers or others. Consumers may also sell their web browsing histories to the Nielson Corporation for up to $50 annually.

100. Because their Private Information has value, Plaintiffs and Class members must take significant protective measures, including years of constant surveillance of their financial and personal records, credit monitoring, and identity protection.

Defendant Could Have Foreseen and Prevented the Data Breach

101. Nothing about this attack was extraordinary. Cybercriminals commonly target the healthcare industry due to the treasure troves of confidential health and personal information maintained and stored by healthcare organizations.

[44] *See 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse*, WASH. POST, Andrea Peterson, Mar. 20, 2015, available at http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 10, 2016).

102. Cyberattacks against the healthcare industry in particular have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals targeting healthcare providers and others were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII."[45]

103. The FBI again warned healthcare stakeholders in 2014 that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[46]

104. In 2017, the Department of Health and Human Services released a ransomware Fact Sheet. This document made it clear to entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[47]

105. Additionally, in light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July

---

[45] Gordon M. Snow, FBI, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, The FBI Testimony (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[46] *See FBI Cyber Bulletin: Malicious Actors Targeting Protected Health Information,* FEDERAL BUREAU OF INVESTIGATION (Aug. 19, 2014) https://publicintelligence.net/fbi-targeting-healthcare20(PII).

[47] *See Fact Sheet: Ransomware and HIPAA,* U.S. DEP'T. OF HEALTH & HUM. SERV'S., https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited June 7, 2024).

2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

106. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into healthcare networks for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[48]

107. Under the HIPAA Privacy Rules, a breach is defined as, "[t]he acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[49] Accordingly, an attack such as the one that was discovered on or about February 21, 2024 is considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule.

108. Such an attack is also considered a "Security Incident" under HIPAA. Under the HIPAA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304. According to the Department of Health

[48] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, THE HIPAA J. (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[49] *See Fact Sheet: Ransomeware and HIPAA*, U.S. DEP'T OF HEALTH & HUM. SERV'S, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited July 3, 2024).

and Human Services, "[t]he presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."[50]

109. Data Breaches can be prevented. Cybersecurity professionals and applicable information security standards urge organizations to take reasonable technical and administrative information security controls. Commonly recommended controls include: ensuring computer networks are adequately segmented, implementing and configuring intrusion prevention and detection technologies, monitoring computer systems using appropriate tools and responding to alerts on suspicious behavior, implementing spam and malware filters, requiring multifactor authentication for external access, implementing secure cryptographic algorithms, timely applying security patches and updates, limiting the use of privileged or administrative accounts, training employees on the handling of suspicious emails, implementing an effective vulnerability management program, ensuring vendors implement and maintain adequate security controls, and implementing heightened security controls around sensitive data sources.

110. The Data Breach underscores Defendants' failure to sufficiently implement one or more vital security measures aimed at preventing cyberattacks. The Data Breach never would have occurred without Defendants' inadequate cybersecurity controls, enabling data thieves to access and acquire the Private Information of hundreds of thousands to millions of individuals, including Plaintiffs and Class members.

111. Defendants knew that unprotected or exposed Private Information in the custody of healthcare companies is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

[50] *See id.*

112. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

113. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendants Did Not Comply with Federal Law and Regulatory Guidance

Defendants did not comply with FTC Guidelines

114. The United States government issues guidelines for businesses that store sensitive data to help them minimize the risks of a data breach. The FTC publishes guides for businesses about the importance of reasonable data security practices.[51] One of its publications sets forth data security principles and practices for businesses to protect sensitive data.[52] The FTC tells businesses to (a) protect the personal information they collect and store; (b) dispose of personal information it no longer needs; (c) encrypt information on their networks; (d) understand their network's vulnerabilities; (e) put policies in place to correct security problems. The FTC recommends businesses use an intrusion detection system, monitor networks for large, outgoing

[51] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (2023), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited June. 7, 2024).

[52] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-informationguide-business (last visited June 7, 2024).

data transmissions, monitor incoming traffic for unusual activity, and make a plan in case a breach occurs.[53]

115. Further, the FTC tells organizations to limit access to sensitive data, require the use of complex passwords on networks, use industry-tested security methods; and verify the use of reasonable security measures by third-party service providers.[54]

116. The FTC brings enforcement actions against businesses that fail to reasonably protect customer information. The Commission treats the failure to use reasonable care and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders issued in these actions state the measures required for businesses to meet their data security obligations.[55]

117. These FTC enforcement actions include actions against healthcare industry companies like Defendants. *See, e.g., In the Matter of LabMd, Inc., A Corp*, No. 9357, 2016 WL 4128215, at *32 (F.T.C. July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act."), vacated on other grounds, *LabMD, Inc. v. Fed. Trade Comm'n,* 894 F.3d 1221 (11th Cir. 2018).

118. Defendants knew of their obligations to implement and use basic data security practices to protect to Plaintiffs' and Class members' Private Information properly.

---

[53] *Id.*
[54] FED. TRADE COMM'N. *supra* n.51.
[55] Privacy and Security Enforcement, FED. TRADE COMM'N., https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited June 7, 2024).

119. Still, Defendants failed to comply with those recommendations and guidelines, which if followed would have prevented the Data Breach. This failure to reasonably protect against unauthorized access to Private Information is an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

120. Defendants' failure to protect Plaintiffs' and Class members' Private Information suggests their failure to comply fully with standard cybersecurity practices such as those described above.

Defendant did not comply with HIPAA Guidelines

121. Defendants provide healthcare, medication, pharmacy, and pharmaceutical related services to hundreds of millions of patients annually either directly or via their healthcare clients. As a regular and necessary part of their businesses, Defendants directly or indirectly collect, store, and transfer the highly sensitive Private Information of patients.

122. As covered entities, Defendants are required under federal and state law to maintain the strictest confidentiality of the Private Information they acquire, receive, collect, transfer, and store. Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

123. Due to the nature of Defendants' businesses, which includes providing a range of drug distribution, patient support services, business analytics and technology, and other services to healthcare clients, including obtaining, storing, and maintaining electronic health and medical records, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information they know and understand to be sensitive and confidential.

124. In fact, whenever Defendants contract with healthcare providers to provide various business and medical services, HIPAA requires that these contracts mandate that Defendants will use adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule[56] and immediately reporting any unauthorized use or disclosure of PHI such as the Data Breach.

125. For their part, Defendants Cencora and Lash Group explicitly tout their commitment to protecting the privacy of Private information, claiming that:

> Cencora, Inc. and its affiliate companies ("Cencora") *value and protect the personal information* entrusted to the company by its suppliers, customers, and visitors. As a United States company doing business around the world, Cencora *maintains a comprehensive privacy program* designed to comply with its legal obligations under applicable law.[57]

126. BMS, GSK, and Cencora articulate similar promises in their respective privacy policies, discussed in detail *supra*.

127. The Data Breach resulted from a combination of multiple failures by the Defendants to adequately and reasonably secure the Plaintiffs' and Class members' Private Information in violation of the mandates set forth in HIPAA's regulations.

Defendant did not comply with Industry Standards

128. Experts in cybersecurity frequently highlight healthcare-related entities as particularly vulnerable to cyberattacks due to the high value of the Private Information they collect and maintain.

---

[56] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. § 160 and § 164, Subparts A and C.

[57] *Privacy Statement Overview*, CENCORA, https://www.cencora.com/global-privacy-statement-overview (last accessed June 20, 2024) (emphasis added).

129. The minimum information security standards applicable to Defendants are established by industry-accepted information security frameworks, including: the NIST Cybersecurity Framework, the Center for Internet Security's Critical Security Controls (CIS CSC), and the HITRUST CSF, which are all established standards in reasonable cybersecurity readiness.

130. The aforementioned frameworks represent established industry standards for healthcare-related entities. Had Defendants complied with these accepted standards, the hackers would not have been able to exploit Defendants vulnerabilities and carry out the Data Breach.

The Data Breach Caused Its Victims Harm

131. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the hands of criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is imminent. Consequently, Plaintiffs and Class members have sustained actual and imminent injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the effects of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures unless Defendants implement appropriate and adequate information security controls.

132. The unencrypted Private Information of Plaintiffs and Class members will almost certainly end up being distributed through illicit underground criminal networks, including being sold on the dark web, as that is the modus operandi of the financially motivated hackers that

perpetrated the Data Breach. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members.

133. As a result of the Data Breach, hackers can now commit identity theft, financial fraud, and other fraud against Plaintiffs and Class members, given the stolen Private Information's sensitive nature. Plaintiffs and Class members therefore have suffered injury and face an imminent, substantial risk of further injuries like identity theft and related cybercrimes.

134. The Private Information likely exposed in the Data Breach is highly valuable and sought after on illicit underground markets for use in committing identity theft and fraud. Malicious actors use this data to access bank accounts, credit cards, and social media accounts, among other things. They may also use the Private Information to open new financial or utility accounts, seek medical treatment using victims' insurance, file fraudulent tax returns, seek and obtain government benefits or government IDs, or create new identities for use in committing frauds. Because victims of breaches can become less diligent in account monitoring over time, bad actors may wait years before using the Private Information, or they may re-use it to commit several cybercrimes.

135. The Government Accountability Office reported that criminals often hold onto stolen data for more than a year after it is obtained, waiting for victims to become less vigilant before using the data to commit identity theft. And fraudulent use of data may continue for years after its sale or publication. The GAO concluded that studies that try to measure harms from data breaches "cannot necessarily rule out all future harm."[58]

[58] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, at 29, U.S. GOV'T. ACCOUNTABILITY OFFICE, http://www.gao.gov/new.items/d07737.pdf (last visited June 7, 2024) ("GAO Report").

136. Even where individuals receive reimbursement for resulting financial losses, they are not made whole again. The Identity Theft Resource Center's 2021 survey reported that victims of identity theft reported suffering negative experiences and emotional harms: anxiety (84%); feelings of violation (76%); rejection for credit or loans (83%); financial related identity problems (32%); resulting problems with family members (32%); feeling suicidal (10%).[59]

137. Physical harms also result from identity theft. A similar survey found that victims suffered resulting physical symptoms: sleep disturbances (48.3%); inability to concentrate / lack of focus (37.1%); inability to work because of physical symptoms (28.7%); new physical illnesses including stomach problems, pain, and heart palpitations (23.1%); starting or relapsing into unhealthy or addictive behaviors (12.6%).[60]

138. Theft of PHI carries significant consequences. A thief could potentially exploit your identity or health insurance details to seek medical treatment, obtain prescription medications, submit claims to your insurance provider, or access other healthcare services. If the thief's health information becomes intertwined with data breach victim's, it can affect victim's medical treatment, insurance coverage, payment records, and even the victim's credit report.

---

[59] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, at 6, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.

[60] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., at 12, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited June 7, 2024).

139. Unauthorized disclosure of sensitive Private Information also reduces its value to its rightful owner, as recognized by courts as an independent source of harm.[61] PHI constitutes a valuable property right.[62]

140. Even consumers who have been victims of previous data breaches are injured when their data is stolen and traded. Each data breach increases the likelihood that the victim's personal information will be exposed on the dark web to more individuals who are looking to misuse it.

141. Because of these injuries resulting from the Data Breach, Plaintiffs and Class members suffer and continue to suffer economic loss and actual harm, including:

- disclosure or confidential information to a third party without consent;
- loss of the value of explicit and implicit promises of data security;
- identity fraud and theft; anxiety, loss of privacy, and emotional distress;
- the cost of detection and prevention measures for identity theft and unauthorized financial account use;
- lowered credit scores from credit inquiries; unauthorized charges;
- diminution of value of PII and PHI;

[61] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[62] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

- loss of use of financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amounts they were permitted to obtain from accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs of credit monitoring, identity theft production services, and credit freezes;
- costs associated with loss of time or productivity or enjoyment of one's life from the time required to mitigate and address consequences and future consequences of the Data Breach, such as searching for fraudulent activity, imposing withdrawal and purchase limits, as well as the stress and nuisance of Data Breach repercussions;
- imminent, continued, and certainly impending injury flowing from the potential fraud and identity theft posed by the unauthorized possession of data by third parties.

142. Plaintiffs and Class members place a significant value on data security. About half of consumers consider data security to be a main or important consideration in their purchasing decisions and would be willing to pay more to work with those with better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[63]

Victims Have Lost the Benefit of the Bargain

143. Furthermore, Defendants' poor data security practices deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendants and/or their

[63] *Beyond the Bottom Line: The Real Cost of Data Breaches,* FIREEYE, p. 14, (May 2016), https://web.archive.org/web/20230628100935/https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf.

agents for the provision of medical services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

144. For the reasons described above, criminals will exploit this Private Information for identity theft crimes, such as opening bank accounts in victims' names for purchases or money laundering, filing fraudulent tax returns, securing loans or lines of credit, or submitting false unemployment claims.

145. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

146. Consequently, Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

147. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per individual. This is reasonable and necessary cost to monitor to protect Plaintiffs and Class members from the risk of identity theft that arose from the Data Breach.

Allegations Relating to Plaintiffs

Plaintiff Juan Anaya's Experience

148. Plaintiff Anaya received a letter dated May 24, 2024, notifying him that the Data Breach had impacted his Private Information, which Lash Group had "processed through its work assisting the GlaxoSmithKline Group of Companies and/or the GlaxoSmithKline Patient Access Programs Foundation."

149. To use GSK and Cencora's services, Plaintiff Anaya—like other Class members—provided sensitive Private Information including his full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to GSK directly or to his healthcare providers or pharmacies to provide to GSK and/or Cencora.

150. GSK and/or Cencora, on GSK's behalf, obtained and continue to store and maintain Plaintiff Anaya's Private Information. GSK and Cencora owe Plaintiff Anaya a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Anaya's Private Information was compromised and disclosed as a result of GSK's and Cencora's inadequate data security practices, which resulted in the Data Breach.

151. Over three months after the Data Breach, GSK and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Anaya's compromised data includes, at minimum: his name, address, date of birth, health diagnosis, and medications and prescription information.

152. Plaintiff Anaya is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Anaya has never knowingly transmitted unencrypted sensitive Private

Information over the internet or any other unsecured source. Plaintiff Anaya would not have entrusted his Private Information to GSK and/or Cencora had he known of their lax data security practices.

153. In response to the Data Breach, Plaintiff Anaya diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

154. Plaintiff Anaya has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of his Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of his Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within GSK's and/or Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

155. The Data Breach has caused Plaintiff Anaya to suffer fear, anxiety, and stress, which has been compounded by the fact that GSK and Cencora have still not fully informed him of key details about the Data Breach's occurrence.

156. As a result of the Data Breach, Plaintiff Anaya anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

157. As a result of the Data Breach, Plaintiff Anaya is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

158. Plaintiff Anaya has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Steven Betts's Experience

159. Plaintiff Betts received a letter dated May 23, 2024, notifying him that the Data Breach had impacted his Private Information, which Lash "has through its partnership with Sumitomo Pharma America, Inc. f/k/a/ Sunovion Pharmaceuticals Inc. in connection with its patient support programs."

160. To use Sumitomo and Cencora's services, Plaintiff Betts—like other Class members—provided sensitive Private Information including his full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to Sumitomo (or Sunovion Pharmaceuticals Inc.) directly or to his healthcare providers or pharmacies to provide to Sumitomo and/or Cencora.

161. Sumitomo or Cencora, on Sumitomo's behalf, obtained and continue to store and maintain Plaintiff Betts's Private Information. Sumitomo and Cencora owe Plaintiff Betts a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Betts's Private Information was compromised and disclosed as a result of Sumitomo's and Cencora's inadequate data security practices, which resulted in the Data Breach.

162. Over three months after the Data Breach, Sumitomo and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Betts's compromised data includes, at minimum: his name, address, date of birth, health diagnosis, and medications and prescription information.

163. Plaintiff Betts is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Betts has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Betts would not have entrusted his Private Information to Sumitomo and/or Cencora had he known of their lax data security practices.

164. In response to the Data Breach, Plaintiff Betts diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

165. Plaintiff Betts has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of his Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure

of his Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Sumitomo's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

166. The Data Breach has caused Plaintiff Betts to suffer fear, anxiety, and stress, which has been compounded by the fact that Sumitomo and Cencora have still not fully informed him of key details about the Data Breach's occurrence.

167. As a result of the Data Breach, Plaintiff Betts anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

168. As a result of the Data Breach, Plaintiff Betts is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

169. Plaintiff Betts has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff William Cook's Experience

170. Plaintiff Cook received a letter dated May 17, 2024, notifying him that the Data Breach had impacted his Private Information, which Lash Group "has through the patient support and access programs it manages on behalf of Bristol Myers Squibb and/or the Bristol Myers Squibb Patient Assistance Foundation."

171. To use BMS and Cencora's services, Plaintiff Cook—like other Class members—provided sensitive Private Information such as his full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card

information, family medical history, and more either to BMS directly or to his healthcare providers or pharmacies to provide to BMS and/or Cencora.

172. BMS and/or Cencora on BMS's behalf obtained and continue to store and maintain Plaintiff Cook's Private Information. BMS and Cencora owe Plaintiff Cook a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Cook's Private Information was compromised and disclosed as a result of BMS's and Cencora's inadequate data security practices, which resulted in the Data Breach.

173. Over three months after the Data Breach, BMS and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Cook's compromised data includes, at minimum: his name, address, date of birth, health diagnosis, and medications and prescriptions information.

174. Plaintiff Cook is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Cook has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Cook would not have entrusted his Private Information to BMS and/or Cencora had he known of their lax data security practices.

175. In response to the Data Breach, Plaintiff Cook diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

176. Plaintiff Cook has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of his Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of his Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within BMS's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

177. The Data Breach has caused Plaintiff Cook to suffer fear, anxiety, and stress, which has been compounded by the fact that BMS and Cencora have still not fully informed him of key details about the Data Breach's occurrence.

178. As a result of the Data Breach, Plaintiff Cook anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

179. As a result of the Data Breach, Plaintiff Cook is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

180. Plaintiff Cook has a continuing interest in ensuring that his Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Amber Hornick's Experience

181. Plaintiff Hornick received a letter dated May 24, 2024, notifying her that the Data Breach had impacted her Private Information, which Lash Group had "processed through its work assisting the GlaxoSmithKline Group of Companies and/or the GlaxoSmithKline Patient Access Programs Foundation."

182. To use GSK and Cencora's services, Plaintiff Hornick—like other Class members—provided sensitive Private Information including her full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to GSK directly or to her healthcare providers or pharmacies to provide to GSK and/or Cencora.

183. GSK and/or Cencora on GSK's behalf, obtained and continue to store and maintain Plaintiff Hornick's Private Information. GSK and Cencora owe Plaintiff Hornick a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Hornick's Private Information was compromised and disclosed as a result of GSK's and Cencora's inadequate data security practices, which resulted in the Data Breach.

184. Over three months after the Data Breach, GSK and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Hornick's compromised data includes, at minimum: her name, address, date of birth, health diagnosis, and medications and prescriptions information.

185. Plaintiff Hornick is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Hornick has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Hornick would not have

entrusted her Private Information to GSK and/or Cencora had she known of their lax data security practices.

186. In response to the Data Breach, Plaintiff Hornick diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

187. Plaintiff Hornick has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within GSK's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

188. The Data Breach has caused Plaintiff Hornick to suffer fear, anxiety, and stress, which has been compounded by the fact that GSK and Cencora have still not fully informed her of key details about the Data Breach's occurrence.

189. As a result of the Data Breach, Plaintiff Hornick anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

190. As a result of the Data Breach, Plaintiff Hornick is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

191. Plaintiff Hornick has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Carolyn Pluhar's Experience

192. Plaintiff Pluhar received a letter dated May 22, 2024, notifying her that the Data Breach had impacted her Private Information, which Lash Group "has through its partnership with one such organization [pharmaceutical companies, pharmacies, and healthcare providers] in connection with its patient support programs." The letter Ms. Pluhar received neglected to identify the company to which Ms. Pluhar had directly given her Private Information which in turn shared her information with Cencora. The identity of this pharmaceutical company is currently within the sole possession Defendants Cencora and Lash Group.

193. To use the services of the unidentified pharmaceutical company and Cencora, Plaintiff Pluhar—like other Class Members—provided sensitive Private Information including her full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to GSK directly or to her healthcare providers or pharmacies to provide to GSK and/or Cencora.

194. The unidentified pharmaceutical company and/or Cencora on that company's behalf obtained and continue to store and maintain Plaintiff Pluhar's Private Information. Both the unidentified pharmaceutical company and Cencora owe Plaintiff Pluhar a legal duty and

obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Pluhar's Private Information was compromised and disclosed as a result of the unidentified pharmaceutical company's and Cencora's inadequate data security practices, which resulted in the Data Breach.

195. Over three months after the Data Breach, the unidentified pharmaceutical company and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Pluhar's compromised data includes, at minimum: her name, address, date of birth, health diagnosis, and medications and prescriptions information.

196. Plaintiff Pluhar is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Pluhar has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Pluhar would not have entrusted her Private Information to the unidentified pharmaceutical company and/or Cencora had she known of their lax data security practices.

197. In response to the Data Breach, Plaintiff Pluhar diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

198. Plaintiff Pluhar has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private

Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within the unidentified pharmaceutical company's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

199. The Data Breach has caused Plaintiff Pluhar to suffer fear, anxiety, and stress, which has been compounded by the fact that the unidentified pharmaceutical company and Cencora have still not fully informed her of key details about the Data Breach's occurrence.

200. As a result of the Data Breach, Plaintiff Pluhar anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

201. As a result of the Data Breach, Plaintiff Pluhar is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

202. Plaintiff Pluhar has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kyle Reynolds's Experience

203. Plaintiff Reynolds received a letter dated May 30, 2024, notifying him that the Data Breach had impacted his Private Information, which Lash which Lash Group "has through its partnership with one such organization [pharmaceutical companies, pharmacies, and healthcare providers] in connection with its patient support programs." The letter Mr. Reynolds

received neglected to identify the company to which Mr. Reynolds had directly given his Private Information which in turn shared his information with Cencora.

204. While confirmation of the identity of this pharmaceutical company is within the possession, custody, or control of Defendants Regeneron, Cencora, and Lash Group, Plaintiff Reynolds has good cause to believe that Defendant Regeneron is the pharmaceutical company that gave his Private Information to Cencora.

205. Plaintiff Reynolds takes only one medication, which he has taken for six years, and this medication is manufactured by Defendant Regeneron.

206. To use Regeneron's and Cencora's services, Plaintiff Reynolds—like other Class members—provided sensitive Private Information including his full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more either to Regeneron directly or to his healthcare providers or pharmacies to provide to Regeneron and/or Cencora.

207. Regeneron and/or Cencora on Regeneron's behalf obtained and continue to store and maintain Plaintiff Reynolds's Private Information. Regeneron and Cencora owe Plaintiff Reynolds a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Plaintiff Reynolds's Private Information was compromised and disclosed as a result of Regeneron's and Cencora's inadequate data security practices, which resulted in the Data Breach.

208. Over three months after the Data Breach, Regeneron and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Reynolds's compromised data includes, at minimum: his name, address, date of birth, health diagnosis, and medications and prescriptions information.

209. Plaintiff Reynolds is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Reynolds has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Reynolds would not have entrusted his Private Information to Regeneron and/or Cencora had he known of their lax data security practices.

210. In response to the Data Breach, Plaintiff Reynolds diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

211. Plaintiff Reynolds has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of his Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of his Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Regeneron's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

212. The Data Breach has caused Plaintiff Reynolds to suffer fear, anxiety, and stress, which has been compounded by the fact that Regeneron and Cencora have still not fully informed him of key details about the Data Breach's occurrence.

213. As a result of the Data Breach, Plaintiff Reynolds anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

214. As a result of the Data Breach, Plaintiff Reynolds is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

215. Plaintiff Reynolds has a continuing interest in ensuring that his Private Information, which remains in Cencora's and Regeneron's possession, is protected and safeguarded from future breaches.

Plaintiff Virginia Romano's Experience

216. Plaintiff Romano received a letter dated May 30, 2024, notifying her that the Data Breach had impacted her Private Information, which Lash Group "has through its partnership with one such organization [pharmaceutical companies, pharmacies, and healthcare providers] in connection with its patient support programs." The letter Ms. Romano received neglected to identify the company to which Ms. Romano had directly given her Private Information which in turn shared her information with Cencora. The identity of this pharmaceutical company is currently within the sole possession Defendants Cencora and Lash Group.

217. To use the services of the unidentified pharmaceutical company and Cencora, Plaintiff Romano—like other Class members—provided sensitive Private Information including her full name, address, date of birth, Social Security number, medical records, insurance

information, billing, banking, and credit card information, family medical history, and more either to GSK directly or to her healthcare providers or pharmacies to provide to GSK and/or Cencora.

218. The unidentified pharmaceutical company and/or Cencora on that company's behalf obtained and continue to store and maintain Plaintiff Romano's Private Information. Both the unidentified pharmaceutical company and Cencora owe Plaintiff Romano a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff Romano's Private Information was compromised and disclosed as a result of the unidentified pharmaceutical company's and Cencora's inadequate data security practices, which resulted in the Data Breach.

219. Over three months after the Data Breach, the unidentified pharmaceutical company and Cencora have yet to confirm the exact information that was compromised in the Data Breach. However, Plaintiff Romano's compromised data includes, at minimum: her name, address, date of birth, health diagnosis, and medications and prescriptions information.

220. Plaintiff Romano is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Romano has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Romano would not have entrusted her Private Information to the unidentified pharmaceutical company and/or Cencora had she known of their lax data security practices.

221. In response to the Data Breach, Plaintiff Romano diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—

time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

222. Plaintiff Romano has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within the unidentified pharmaceutical company's and Cencora's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

223. The Data Breach has caused Plaintiff Romano to suffer fear, anxiety, and stress, which has been compounded by the fact that the unidentified pharmaceutical company and Cencora have still not fully informed her of key details about the Data Breach's occurrence.

224. As a result of the Data Breach, Plaintiff Romano anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

225. As a result of the Data Breach, Plaintiff Romano is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

226. Plaintiff Romano has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

227. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs propose the following "Class" definition, subject to amendment as appropriate:

> **Nationwide Class:**
> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred in or about February 2024, including all persons who were sent a notice of the Data Breach. (the "Class").

228. Plaintiffs also seek certification of the following statewide subclasses, defined as follows and subject to amendment as appropriate:

> **BMS Subclass:**
> All persons whose Private Information was provided to BMS or to Cencora at BMS's behest to receive services from BMS and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach (the "BMS Subclass").
>
> **GSK Subclass:**
> All persons whose Private Information was provided to GSK or to Cencora at GSK's behest to receive services from GSK and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach (the "GSK Subclass").
>
> **Regeneron Subclass:**
> All persons whose Private Information was provided to Regeneron or to Cencora at Regeneron's behest to receive services from Regeneron and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach (the "Regeneron Subclass").
>
> **Sumitomo Subclass:**
> All persons whose Private Information was provided to Sumitomo or to Cencora at Sumitomo's behest to receive services from Sumitomo and was accessed in the Data Breach by unauthorized persons, including all such

persons who were sent a notice of the Data Breach (the "Sumitomo Subclass").

229. Excluded from the Class are the following individuals and/or entities: Cencora and Cencora's parents, subsidiaries, affiliates, officers and directors, and any entity in which Cencora has a controlling interest; Lash Group and Lash Group's parents, subsidiaries, affiliates, officers and directors, and any entity in which Lash Group has a controlling interest; BMS and BMS's parents, subsidiaries, affiliates, officers and directors, and any entity in which BMS has a controlling interest; GSK and GSK's parents, subsidiaries, affiliates, officers and directors, and any entity in which GSK has a controlling interest; Regeneron and Regeneron's parents, subsidiaries, affiliates, officers and directors, and any entity in which Regeneron has a controlling interest; Sumitomo and Sumitomo's parents, subsidiaries, affiliates, officers and directors, and any entity in which Sumitomo has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, members of their immediate families, and chambers staff.

230. Plaintiffs reserve the right to amend the definitions of the Class or add additional Classes or Subclasses.

231. Numerosity: The patients of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Cencora, at least 500,000 individuals were impacted. The Class is apparently identifiable within Cencora's records, and Cencora has already identified many of these individuals (as evidenced by sending them breach notification letters). As of May 28, 2024 at least 500,000 affected individuals had been notified,

but the actual number of victims could be much higher considering that Cencora has serviced over 18 million customers to date.[64]

232. Commonality: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiffs and Class members for non-business purposes;

d. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Private Information

e. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class members;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether and when Defendants actually learned of the Data Breach;

h. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information had been compromised;

[64] Krishi Chowdhary, *Major Pharmaceutical Companies Hit by Data Breach Linked to Cencora Cyberattack*, TECHREPORT (May 28, 2024), https://techreport.com/news/major-pharmaceutical-companies-data-breach-cencora-cyberattack/.

i. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their Private Information had been compromised;

j. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants breached implied contracts with Plaintiffs and Class members;

n. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class members;

o. Whether Plaintiffs and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

p. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

233. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had Private Information compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

234. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class members uniformly and Plaintiffs' challenges of these policies hinge on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

235. Adequacy: Plaintiffs will serve as fair and effective representatives for the Class members, possessing no conflicting interests that would hinder the protection of their rights. The relief sought by the Plaintiffs aligns with the collective interests of the Class, without any adverse implications for its members. The infringements upon the Plaintiffs' rights and the damages incurred are emblematic of those experienced by other Class members. Moreover, Plaintiffs have engaged legal counsel adept in navigating intricate class action and data breach litigation, demonstrating a commitment to vigorously pursue this case.

236. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

237. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

238. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

239. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

240. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class members, Defendants may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

241. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

242. Similarly, specific issues outlined in Rule 42(d)(1) warrant certification as they entail distinct yet shared concerns pivotal to advancing the resolution of this case and the interests of all parties involved. These issues include, but are not confined to:

a. Whether the Defendants failed to promptly notify both Plaintiffs and the Class about the Data Breach;

b. Whether the Defendants bore a legal responsibility to exercise due diligence in the acquisition, storage, and protection of Private Information belonging to Plaintiffs and the Class;

c. Whether the security measures implemented by Defendants to safeguard their data systems aligned with industry best practices endorsed by data security experts;

d. Whether Defendants' omission of adequate protective security measures amounted to negligence;

e. Whether Defendants neglected to undertake commercially reasonable measures to secure Private Information; and

f. Whether adherence to data security recommendations outlined by the FTC, by HIPAA, and those advocated by data security experts could have feasibly prevented the occurrence of the Data Breach

CAUSES OF ACTION

COUNT I
Negligence
On Behalf of Plaintiffs and the Class

243. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

244. Defendants require consumers, including Plaintiffs and Class members, to submit non-public Private Information, either directly or indirectly, in the ordinary course or providing their services.

245. Defendants gathered and stored the Private Information of Plaintiffs and Class members as part of their business of soliciting their services to their patients, which solicitations and services affect commerce.

246. Plaintiffs and Class members entrusted Defendants with their private information, expecting that Defendants would protect and secure it.

247. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

248. By voluntarily undertaking the responsibility to collect, store, share, and use this data for commercial gain, Defendants assumed a duty of care to employ reasonable measures to secure and safeguard their computer systems and the Private Information of Class members contained within them. This duty included preventing unauthorized disclosure and protecting the information from theft. Additionally, Defendants were responsible for implementing processes to detect security breaches promptly and to notify affected individuals expeditiously in the event of a data breach.

249. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

250. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

251. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks adequately protected the Private Information.

252. Defendants' duty to employ reasonable security measures arose from the special relationship between Defendants and Plaintiffs and Class members. This relationship was established because the Plaintiffs and Class members entrusted Defendants with their confidential private information, both directly and indirectly as a necessary part of being consumers of the services provided by and the medications produced and/or distributed by Defendants.

253. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

254. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

255. Defendants also had a duty to exercise appropriate data deletion practices to remove former consumers' Private Information they were no longer required to retain pursuant to regulations.

256. Defendants had, and continue to have, a duty to adequately disclose if the Private Information in their possession might have been compromised, the manner in which it was compromised, the specific types of data affected, and the timing of the breach. Such notice is necessary to enable the Plaintiffs and Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their private information by third parties.

257. Defendants breached their duties under the FTC Act, HIPAA, and other relevant standards, demonstrating negligence by failing to implement reasonable measures to protect Class members' Private Information. Specific negligent actions and oversights by the Defendants include, but are not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Class members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Class members' Private Information.

d. Failing to promptly detect that Class members' Private Information had been compromised.

e. Neglecting to remove Private Information of former patients or customers that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Class members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

258. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given

the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

259. Plaintiffs and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

260. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

261. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

262. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

263. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

264. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems or transmitted through third party systems.

265. It was thus foreseeable that the failure to adequately safeguard Class members' Private Information would lead to one or more forms of harm or injury to the Class members.

266. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

267. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

268. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship.

269. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

270. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

271. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

272. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

273. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

274. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

275. Plaintiffs and the Class are also entitled to injunctive relief, which should compel the Defendants to implement and maintain reasonable and adequate technical and administrative information security controls given the vast amounts of extremely sensitive Private Information they collect, process, and store.

COUNT II
Negligence Per Se
On Behalf of Plaintiffs and the Class

276. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

277. According to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants were obligated to furnish fair and adequate computer systems and data security practices to protect the private information of both the Plaintiffs and Class members.

278. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

279. Defendants breached their duties to Plaintiffs and Class members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

280. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

281. Plaintiffs and Class members are within the class of persons the statutes were intended to protect and the harm to Plaintiffs and Class members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

282. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

283. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that by failing to meet their duties, Defendants' breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

284. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
On behalf of the Class, against Cencora
On Behalf of the BMS Subclass, against BMS
On Behalf of the GSK Subclass, against GSK
On Behalf of the Regeneron Subclass, against Regeneron
On behalf of the Sumitomo Subclass, against Sumitomo

285. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

286. All Plaintiffs bring this claim, individually and on behalf of the Class against Defendants Cencora, Inc. and The Lash Group LLC.

287. Plaintiff Cook brings this claim, individually and on behalf of the BMS Subclass, against Defendants Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc.

288. Plaintiffs Anaya and Hornick bring this claim, individually and on behalf of the GSK Subclass, against Defendants GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation.

289. Plaintiff Reynolds brings this claim, individually and on behalf of the Regeneron Subclass, against Defendant Regeneron Pharmaceuticals, Inc.

290. Plaintiff Betts brings this claim, individually and on behalf of the Sumitomo Subclass, against Defendant Sumitomo Pharma America, Inc.

291. These Plaintiffs and Subclass members gave, directly or indirectly, the Drug Companies Defendants and Cencora their Private Information in confidence, believing that Drug

Companies Defendants would protect that information. Plaintiffs and Subclass members would not have provided Drug Companies Defendants or Cencora with this information had they known it would not be adequately protected. Drug Company Defendants' acceptance and storage of Plaintiffs' and Subclass members' Private Information created a fiduciary relationship between the Drug Company Defendants and their respective Plaintiffs and Subclass members. In light of this relationship, the Drug Company Defendants must act primarily for the benefit of their current and former patients or customers, which includes safeguarding and protecting Plaintiffs' and Subclass members' Private Information.

292. Drug Company Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Subclass members upon matters within the scope of their relationship. Drug Company Defendants breached that duty by failing to, or contracting with companies that failed to, properly protect the integrity of the system(s) containing Plaintiffs' and Subclass members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Subclass members' Private Information that it collected and maintained.

293. As a direct and proximate result of Drug Company Defendants' breaches of their fiduciary duties, Plaintiffs and Subclass members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Drug Company Defendants' possession; (vi) future costs in terms

of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
Breach of Implied Contract
On behalf of the Class, against Cencora
On Behalf of the BMS Subclass, against BMS
On Behalf of the GSK Subclass, against GSK
On Behalf of the Regeneron Subclass, against Regeneron
On behalf of the Sumitomo Subclass, against Sumitomo

294. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

295. All Plaintiffs bring this claim, individually and on behalf of the Class against Defendants Cencora, Inc. and The Lash Group LLC.

296. Plaintiff Cook brings this claim, individually and on behalf of the BMS Subclass, against Defendants Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation, Inc.

297. Plaintiffs Anaya and Hornick bring this claim, individually and on behalf of the GSK Subclass, against Defendants GlaxoSmithKline, LLC and GlaxoSmithKline Patient Access Programs Foundation.

298. Plaintiff Reynolds brings this claim, individually and on behalf of the Regeneron Subclass, against Defendant Regeneron Pharmaceuticals, Inc.

299. Plaintiff Betts brings this claim, individually and on behalf of the Sumitomo Subclass, against Defendant Sumitomo Pharma America, Inc.

300. In connection with receiving medications or medical services, Plaintiffs and Subclass members entered into implied contracts with the Drug Company Defendants.

301. Pursuant to these implied contracts, Plaintiffs and Subclass members paid money to Drug Company Defendants, whether directly or through their insurers (and/or pharmacies), and provided Drug Company Defendants with their Private Information. In exchange, Drug Company Defendants agreed to and Plaintiffs and Subclass members understood that Drug Company Defendants would, among other things: (1) provide medications or medical services to Plaintiffs and Subclass members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Subclass members' Private Information; and (3) protect Plaintiffs' and Subclass members' Private Information in compliance with federal and state laws and regulations and industry standards.

302. The protection of Private Information was a material term under the implied contracts between Plaintiffs and Subclass members, on one hand, and their respective Drug Company Defendant on the other hand. Had Plaintiffs and Class members known that Drug Company Defendants would not adequately protect their current and former customers' Private Information, they would not have sought healthcare services from Drug Company Defendants.

303. Plaintiffs and Subclass members performed their obligations under the implied contract when they provided Drug Company Defendants with their Private Information and paid—directly or indirectly—for medications, health care or other services from Drug Company Defendants.

304. Drug Company Defendants breached their obligations under their implied contracts with Plaintiffs and Subclass members in failing to implement and maintain reasonable security measures to protect and secure their Private Information and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Subclass members' Private Information in a manner that complies with applicable laws, regulations, and industry standards.

305. Drug Company Defendants' breach of their obligations under their implied contracts with Plaintiffs and Subclass members directly resulted in the Data Breach and the injuries that Plaintiffs and Subclass members have suffered from the Data Breach.

306. Plaintiffs and all other Subclass members were damaged by Drug Company Defendants' breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
Unjust Enrichment
On Behalf of Plaintiffs and the Class

307. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

308. Additionally or in the alternative, Plaintiffs and the Class bring this claim for unjust enrichment.

309. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they paid Defendants, either directly or indirectly, for the provision of medications and/or services and in so doing also provided Defendants with their Private Information. In

exchange, Plaintiffs and Class members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

310. Defendants knew that Plaintiffs and Class members conferred a benefit upon it and had accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendants profited from Plaintiffs' and Class members' retained data and used Plaintiffs' and Class members' Private Information for business purposes.

311. Defendants failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not fully compensate Plaintiffs or Class members for the value that their Private Information provided.

312. Defendants acquired the Private Information through inequitable record retention, having failed to investigate and/or disclose the inadequate data security practices previously mentioned.

313. If Plaintiffs and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendants or obtained services from Defendants.

314. Plaintiffs and Class members have no adequate remedy at law.

315. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants calculated to increase their own profit at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit.

Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of Plaintiffs' and Class members Private Information.

316. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred upon them.

317. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

318. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

319. Plaintiffs and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI

Third-Party Beneficiary Claim for Breach of Contract

On Behalf of Plaintiffs and the Class, against Cencora and Lash Group

320. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

321. Defendants Cencora and Lash Group entered into a contract to provide services to Plaintiffs' and Class members' pharmacies, pharmaceutical companies, healthcare providers, or patient support programs. Upon information and belief, this contract is virtually identical to the contracts entered into between Cencora/Lash Group and their other medical or pharmacy provider customers around the country whose patients were also affected by the Data Breach.

322. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that Defendants agreed to collect and protect through their services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

323. Cencora and Lash Group knew that if they were to breach these contracts with their customers, the customers' patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

324. Cencora and Lash Group breached their contracts with Plaintiffs' and Class Members' pharmacies, pharmaceutical companies, healthcare providers, or patient support programs affected by this Data Breach when they failed to use reasonable data security measures that could have prevented the Data Breach.

325. As foreseen, Plaintiffs and the Class were harmed by Cencora's and Lash Group's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information, increased out-of-pocket medical expenses, and loss of access to medications and/or healthcare treatment and other services.

326. Accordingly, Plaintiffs and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT VII
Declaratory Judgment
On Behalf of Plaintiffs and the Class

327. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

328. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

329. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendants' data security measures remain inadequate, contrary to Defendants' assertion that they have confirmed the security of their networks. Furthermore, Plaintiffs and Class members continue to suffer injury as a result of the compromise of Private Information and remain at imminent risk that further compromises of Private Information will occur in the future.

330. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure Private Information and to timely notify patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and

b. Defendants continue to breach their legal duty by failing to employ reasonable measures to secure consumers' Private Information.

331. This Court also should issue corresponding prospective injunctive relief requiring Defendants to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Plaintiffs' and Class members' Private Information possessed by Defendants; and 3) provide, at their own expense, all impacted victims with lifetime identity theft protection services.

332. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

333. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

334. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. Certifying this action as a class action pursuant to Rule 23, certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class members;

C. Awarding injunctive relief requested by Plaintiffs, including injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including an order:

   i. requiring Defendants to conduct regular database scanning and securing checks;

   ii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as

well as protecting the personal identifying information of Plaintiffs and Class members;

iii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

iv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

v. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

vi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. Awarding Plaintiffs and Class members damages, including actual, nominal, statutory, consequential, and punitive damages, for each cause of action as allowed by law in an amount to be determined at trial;

E. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

F. Awarding Plaintiffs the costs and disbursements of the action, along with reasonable attorney's fees, costs, and expenses;

G. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest at the maximum legal rate;

H. Awarding Plaintiffs and the Class such other favorable relief as allowable under law; and

I. Granting all other such relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all claims so triable.

Date: July 8, 2024

Respectfully submitted,

/s/ Jeannine M. Kenney
Jeannine M. Kenney (PA Bar Id. 307635)
HAUSFELD LLP
325 Chestnut Street, Suite 900
Philadelphia, PA 19106
Tel: (215) 985-3270
Fax: (215) 985-3271
jkenney@hausfeld.com

David M. Berger*
Rosemary Rivas*
Linda Lam*
Sarah E. Hillier*
GIBBS LAW GROUP LLP
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: (510) 350-9700
dmb@classlawgroup.com

rmr@classlawgroup.com
lpl@classlawgroup.com
seh@classlawgroup.com

**pro hac vice applications forthcoming*

Counsel for Plaintiffs and
the Proposed Class